Peeking in on Privacy

Recent Developments in Privacy Law

Canadian Franchise Association National Convention | 14 April 2015

David Elder | Stikeman Elliott LLP
Agenda

1. Legislative Developments
2. Privacy Commissioner Findings
3. Jurisprudence
4. OPC Consultation
5. CASL Developments
Legislative Update

Peeking in on Privacy
S-4

Second Session, Forty-first Parliament,
62-63 Elizabeth II, 2013-2014

SENATE OF CANADA

BILL S-4

An Act to amend the Personal Information Protection and
Electronic Documents Act and to make a consequential
amendment to another Act

AS PASSED
BY THE SENATE
JUNE 16, 2014

S-4

Deuxième session, quarante et unième législature,
62-63 Elizabeth II, 2013-2014

SÉNAT DU CANADA

PROJET DE LOI S-4

Loi modifiant la Loi sur la protection des renseignements
personnels et les documents électroniques et une autre loi
en conséquence

ADOPTÉ
PAR LE SÉNAT
LE 16 JUIN 2014
Bill S-4 – The Digital Privacy Act

The Good

- Broader exemption for “business contact information”
- Explicit recognition of “work product information”
- Enhanced employer rights
- Explicit exemption for information shared or transferred in the course of a business transactions (M&A, financing, etc.)
Bill S-4 – The Digital Privacy Act

The Not So Good

- Compliance agreements
  - Forestalls ability of OPC to apply to Fed Ct, but individual right to apply unaffected
  - Concern re jurisdiction creep
- 1 year for complainants or OPC to apply to Federal Court
  - Currently only 45 days
Bill S-4 – The Digital Privacy Act

The Bad

- Enhanced, but vague consent requirement
  - Designed to better protect vulnerable groups, particularly minors, but worded more broadly
- Record keeping requirement for security breaches – even those not reportable – and provide to OPC on request
- Open-ended power of OPC to disclose any information received from organizations
The Necessary

Mandatory breach notification
  - Requirement to notify OPC and individual
  - Where “creates a real risk of significant harm to an individual”
  - Concern too many need be reported to OPC
  - New offence
2014 Bill 3

Third Session, 28th Legislature, 63 Elizabeth II

THE LEGISLATIVE ASSEMBLY OF ALBERTA

BILL 3

PERSONAL INFORMATION PROTECTION AMENDMENT ACT, 2014

MR. QUADRI

First Reading .................................................................
Second Reading ...........................................................
Committee of the Whole ..................................................
Third Reading .............................................................
Royal Assent ...............................................................
Notable Privacy Commissioner Findings & Initiatives

Peeking in on Privacy
Joint Initiatives

- GPEN Internet Sweep 2014 – focus on mobile apps
- Guidelines for Online Consent
- Joint Open Letter to App Marketplaces – ensure all listed apps have privacy policy links
- Joint letter to Insecam.com – take down site
- Revised MOU between federal, Alberta and BC Commissioners re collaboration and coordination re enforcement, policy, information sharing, education and compliance resources
Notable OPC Findings

- #2014-001: Use of sensitive health information for targeting of Google ads raises privacy concerns
- #2014-003: Insurance company overhauls its security safeguards following privacy breach
- #2014-004: Online service provider that suffered a breach had appropriate safeguards in place
- #2014-007: Apple called upon to be more open about its collection and use of information for downloads
- #2014-008: Agreement to an app’s “permissions” does not, by itself, equal consent to collection, use and disclosure
- #2014-009: Gaps in Microsoft’s Accountability impede response to customer’s privacy complaint
Collecting from Kids

1. Limit collection of personal information – or avoid altogether
2. Be careful about “inadvertent” collection
3. Have an appropriate retention schedule for inactive accounts
4. Speak to the specific services provided to youth
5. Make sure target users can understand – or know how to engage their parents/guardians
6. Consider the user experience
7. Make clear who is agreeing to terms and conditions
8. Ensure you have proper defaults for age of users
9. Know what is happening on your site
10. Prevention is better than monitoring
April 2014 report on employment-related criminal records checks led to revised government policy.

Finding that tokenized government data can be stored outside Canada, notwithstanding FIPPA – lesson for private sector?

Statement re use of employee monitoring software by public bodies (lesson for private sector?):
- Even with notification, must be reasonable or necessary
- Covert assessed on case-by-case basis – but none OK to date

Also reminder to public bodies re video or audio surveillance – only permitted if authorized by law and clear less privacy-invasive options will not be effective (another lesson?)
Consumer Choice Awards Order P2014-02: Award organization disclosed personal information re commenter/complainant to subject organization
In two decision respecting wireless telephone companies (or retail franchisees), the CAI asserted its jurisdiction over telecommunications companies – which are federally regulated

- Can review personal identification information to verify identity, but can’t record numbers (SIN, DLN, etc.) – even with consent of the individual
Jurisprudence

Peeking in on Privacy
Civil Litigation

- Privacy litigation is on the rise
- More individual actions, but damages still relatively low (less than $21,000)
- Trend toward tort actions for invasion of privacy/intrusion upon seclusion
- Tort not recognized in all provinces, particularly where is a statutory cause of action for invasion of privacy (BC, Saskatchewan, Manitoba, Newfoundland & Labrador)
- Court grappling with whether available where other statutory remedy (including damages) available
- Low individual damages can multiply rapidly in class action scenario
The Rise of Class Actions

- *Condon v. Canada*, 2014 FC 250 – lost USB key and hard drive with PI re 583,000 student loan recipients – certified

- *Douez v. Facebook*, 2014 BCSC 953 – use of names and images in “Sponsored Stories” without consent – est. 1.8 million in class - certified

- *Sofio c. IIROC*, 2104 QCCS 4061 – lost encrypted laptop with info on 52,000 brokerage clients – not certified – no actual harm

- *Broutzas v. Rouge Valley Centenary*, 2014 – info for up to 14,000 patients disclosed to RESP marketing companies - $412 million class action pending
The Rise of Class Actions

- Home Depot, 2014 – hacking breach affecting 56 million customers - $500 million proposed class action
- Evans v. Bank of Nova Scotia, 2014 ONSC 2135 – employee provided PI to third parties resulting in fraud – first certified class action for intrusion upon seclusion in Ontario
Charter Cases

  - Canadians have a reasonable expectation of privacy in their use of the internet
  - Police investigation does not, by itself, constitute “lawful authority” to obtain personal information without a warrant
  - S. 7(3)(c.1) of PIPEDA does not create lawful authority, it allows for it from other sources
  - Contractual provisions at issue “confusing and equivocal” re reasonable expectation of privacy re voluntary police requests
  - Police request to an ISP to voluntarily disclose customer information = “search”
Stuck In The Middle With You

- **Equustek Solutions v. Jack, 2014 BCSC 1063**
  - B.C.S.C. orders Google (non-party in IP litigation) to remove specified URLs from its search results **worldwide**

- **Voltage Pictures LLC v. John Doe, 2014 FC 161**
  - ISP ordered to disclose contact information of 2,000 customers to film production company alleging illegal downloads of copyright protected films
  - But with new conditions/safeguards
OPC Consultations
Peeking in on Privacy
OPC Consultations

- New Commissioner held series of consultations (5 cites, Jan-Feb 2015) to obtain input on strategic priorities for coming years
- Suggested issues for discussion:
  1. Economics of personal information
  2. Government services and surveillance
  3. Protecting Canadians in a borderless world
  4. Reputation & privacy
  5. The body as information
  6. Strengthening accountability & privacy safeguards
CASL – The First 9 Months

Peeking in on Privacy
CASL in a Nutshell

Commercial Electronic Messages
- Prohibits sending commercial electronic messages without express consent
- Some exceptions

Installation of Computer Programs
- Prohibits the installation of a computer program without express consent
- Some exceptions

Alteration/Rerouting
- Prohibits the alteration of transmission data or rerouting of messages without express consent
Enforcement

- AMPs for “violations” (Up to $1 M individual, $10 M corporate)
- Undertakings
- Public shaming
- Registration with court – enforced as contempt
- Injunctions, Restraining Orders
- Offences
- Private right of action
- Preservation demand
- Notice to produce
- Search warrant
Spam Reporting Centre up and running

CRTC has received over 250,000 complaints since July 1

Bulk of these were forwarded to spam@fightspam.gc.ca

About 25% filled out online form, provided details
CRTC has been active with respect to enforcement/investigations re CEMs and alteration of transmission data.

- Tools:
  - Preservation demands
  - Notice to produce
  - Warrants

- “Honeypots”

- For computer programs, initial focus on malware/botnets?
CRTC works with small business to stop malicious spam from being sent to Canadians

October 7, 2014 – Ottawa-Gatineau - Canadian Radio-television and Telecommunications Commission (CRTC)

The Canadian Radio-television and Telecommunications Commission (CRTC) announced today that by working with a small Saskatchewan business, it has stopped malicious spam messages from being sent to Canadians. Millions of spam messages were unknowingly being sent from a server owned by a Saskatchewan-based computer reseller.

In July 2014, the Spam Reporting Centre received reports of spam messages routed through Access Communications, an Internet service provider (ISP). During its investigation, the CRTC discovered that the spam messages were actually coming from a small business’s server, which used Access Communications as its ISP. This business’s server had become infected with malware, which had caused it to join the botnet “Ebury.” It is estimated that the infected server had sent millions of malicious spam messages without the business’s or Access Communications’ knowledge.

Once alerted to the situation by the CRTC, the small business and Access Communications fully cooperated and removed all traces of the malware.

According to spamrankings.net, the Autonomous Systems (AS21804) for Access Communications, which includes the small business in question, topped the charts for spam activity in Canada in June and July 2014, peaking at approximately 24 million emails sent in June and 73 million in July. After notification from the CRTC and the action taken by the small business and Access Communication, the activity dropped down to the 36th spot on the spamrankings.net list. The Spam Reporting Centre also stopped receiving spam reports regarding this matter.

By working together and acting swiftly on the reports that came into the Spam Reporting Centre, the CRTC, the Saskatchewan-based small business and Access Communications were able to prevent millions of additional and unwanted spam messages from being sent, reducing the potential harm these messages may have caused Canadians.

The CRTC is assessing all complaints submitted to the Spam Reporting Centre that are under its mandate and a number of
CRTC Chief Compliance and Enforcement Officer issues $1.1 million penalty to Compu-Finder for spamming Canadians

March 5, 2015 – Ottawa-Gatineau - The Canadian Radio-television and Telecommunications Commission’s (CRTC’s) Chief Compliance and Enforcement Officer today issued a Notice of Violation to Compu-Finder, which includes a penalty of $1.1 million, for breaking Canada’s anti-spam law. Compu-Finder has 30 days to submit written representations to the CRTC or pay the penalty. It also has the option of requesting an undertaking with the CRTC on this matter.

Further to an investigation, the Chief Compliance and Enforcement Officer finds that Compu-Finder sent commercial electronic messages without the recipient’s consent as well as emails in which the unsubscribe mechanisms did not function properly. The emails sent by Compu-Finder promoted various training courses to businesses, often related to topics such as management, social media and professional development. The four alleged violations occurred between July 2, 2014 and September 16, 2014. Furthermore, an analysis of the complaints made to the Spam Reporting Centre of this industry sector shows that Compu-Finder accounts for 26% of all complaints submitted.

The CRTC is assessing complaints submitted to the Spam Reporting Centre that are under its legislative mandate and a number of investigations are currently underway. The CRTC is working with its partners, both within Canada and internationally, to protect Canadians from online threats and contribute to a more secure online environment.

The CRTC can discuss corrective actions with individuals, firms or organizations, which may lead to an undertaking that includes an amount to be paid and other corrective measures. As part of its powers, the CRTC can also issue warning letters, preservation demands, notices to produce, restraining orders and notices of violation.

Canadians are encouraged to report spam to the Spam Reporting Centre. The information sent to the Centre is used by the CRTC, the Competition Bureau, and the Office of the Privacy Commissioner to enforce Canada’s anti-spam law.
Plentyoffish Media Inc. pays $48,000 for alleged violation of Canada's anti-spam law


The Canadian Radio-television and Telecommunications Commission (CRTC) today announced that Plentyoffish Media Inc. has paid $48,000 as part of an undertaking for an alleged violation of Canada’s anti-spam legislation.

Acting on complaints submitted by Canadians, the CRTC’s Chief Compliance and Enforcement Officer launched an investigation. Plentyoffish Media had allegedly sent commercial emails to registered users of the Plenty of Fish online dating service with an unsubscribe mechanism that was not clearly and prominently set out, and which could not be readily performed, as required by the legislation. The emails sent by Plentyoffish Media notified users of services available through their registration to the dating site. The alleged violation occurred between July 1, 2014 and October 8, 2014.

Once made aware of the investigation by the CRTC, Plentyoffish Media updated its unsubscribe mechanism to comply with the legislation.

As part of the undertaking, Plentyoffish Media will develop and implement a compliance program to ensure that its activities are compliant with Canada’s anti-spam legislation. The compliance program will include training and education for staff and corporate policies and procedures.

The CRTC is assessing all complaints submitted to the Spam Reporting Centre that are under its mandate and a number of investigations are currently underway. The CRTC is working with its partners, both within Canada and internationally, to protect Canadians from online threats and contribute to a more secure online environment.
Installation of Computer Program

- Must not install/cause to be installed a “computer program” on other’s “computer system”
- Installed program must not cause electronic message to be sent from computer system
- Unless:
  - Express consent of owner/authorized user
    - Provide electronic address for remove/disable – for 1 year
    - Provide no-cost assistance re remove/disable request
  - Acting pursuant to court order
Deemed Consent
Cookies
Html Code
JavaScripts
Operating System
Executable only with program installed with consent
TSP programs to protect or upgrade network
Solely to correct a failure

Express Consent
Must set out clearly:
Purpose for consent
Installer identification
General Description of program function and purpose

Enhanced Consent
In addition to Express Consent:
Separate from licence agreement
Detailed description of material elements, including likely impact on user
Greater prominence
Explicit agreement form user to "unexpected functions"
I accept the Terms and Conditions.

I agree to the installation of Company Inc.’s Product A software. The function and purpose of Product A are to request removal or disabling of this computer program under certain conditions, please contact us at this electronic address.

I agree to receive Company Inc.’s newsletter containing news, updates and promotions regarding Company Inc.’s products. You can withdraw your consent at any time. Please refer to our Privacy Policy or Contact Us for more details.
Express Consent – “Enhanced”

For programs that perform certain “unexpected” functions, enhanced disclosure required:

- Interfering with owner/user control of computer
- Collection of personal info stored on computer
- Changing/interfering with settings, preferences or commands – without knowledge of owner/user
- Changing/interfering with data stored on computer so as to interfere with “lawful access” to or use of data
- Unauthorized communication with other computer, device
- Capability of unknown/unauthorized 3rd party activation

Must bring to attention of user separately from any other information in a request for consent, must obtain written acknowledgement that they understand and agree to these functions
Self-Installed Programs

Law **does not apply** where owner or authorized user initiates installation of program on their device:

- Provided that the installation does not include undisclosed programs, unexpected functions
- Includes app store, online, disk-based installations
- Manufacturers and vendors can “self-install” programs on devices before sale to consumers – no further formal consent required from consumer, but disclosures expected
Law will apply where:

- Undisclosed program included with user-initiated download/installation
- Program performs unexpected functions
- What is considered to be “unexpected” will depend on context, including nature of program being installed, disclosures made by developer/distributor
Updates and Upgrades

- Law applies equally to upgrades and updates, including to programs previously installed by user, or pre-installed by manufacturer/vendor
- Must be automatically installed; law doesn’t apply where user initiates
- Law does allow for consent in advance to future automatic updates/upgrades
Grandfathering

For programs installed on a person’s computer system before January 15, 2015:

- Consent to the installation of and update or upgrade is implied until January 15, 2018
- Unless the person provides notice that they no longer consent to receiving such installations
Implementation Checklist

Current & Future

☑️ Watch for further guidance re interpretation re CEMs and program installation

☑️ Careful review of disclosures re program

☑️ Highlight and explain any “unexpected” functions

☑️ Get advance consent to future installation of upgrades/updates (or notify and allow user to install)

☑️ Clear disclosures to consumers where “self-install” by vendor/manufacturer

☑️ Ensure records are retained and retrievable, including online disclosures soliciting consent
Questions and Answers

David Elder
delder@stikeman.com